Follow us On Twitter

DELAWARE DEPARTMENT OF TECHNOLOGY & INFORMATION

June 2014 Issue

SECURITY - Now ...more than ever!

Cyber Security - Disaster Recovery - Continuity of Government

DTI eSecurity News — Unintended Information Disclosure - Updated

Exposing Information

Unintended disclosure is the accidental disclosure of protected information. This includes credit card numbers, social security numbers, medical records, or other personally identifiable information.

Disclosed information exposes data that can be used for identity theft or extortion. It could also be used for an attack on infrastructure systems operated by the government, utility, chemical, finance, transportation, and telecommunication sectors.

Unfortunately in today's digital environment, one of the most common causes of unintended disclosure is a retailer being the victim of a hack attack.

What can I do?

- Protect data with encryption and access controls when appropriate, and adequately erase or destroy electronic storage devices.
- When disposing of confidential documents, use a shredder instead of recycle bins or trash cans.
- Keep portable data storage devices like tablets, laptops, phones, flash drives, in secure locations.

Am I exposing confidential information?

Do you auto-forward your corporate email to other mail systems? Do you use services like Google Docs and Dropbox to store non-public data?

If you answered YES to either of these questions, you are exposing confidential data.

Corporate data with a classification above Public should be stored only on corporate owned systems or on systems under contract. For this reason, auto-forwarding of emails to other email systems creates a significant risk for you, your organization, and the data that you protect.

Additionally, services that offer data storage on internet-based servers, for accessibility while off your corporate network should be used ONLY for public data.

eBay Hack!

The Federal Trade Commission (FTC) suggests taking these steps to protect yourself from potential fraud from the recent eBay hack.

- **Change your eBay password.** When you create your new password, keep these tips in mind.
- **If you used your eBay ID or password for other accounts, change them too.** Hackers sometimes try stolen IDs and passwords on different websites to gain control of other accounts.
- **Don't confirm or provide personal information in response to an email or text, and don't click on links in unexpected messages.** Legitimate companies won't ask for bank or credit card information, social security numbers, passwords, or other sensitive information through unsecured channels. According to news reports, the eBay breach included customers' names, passwords, email and postal addresses, phone numbers, and dates of birth. Crooks may use this stolen information to send you email or text messages that appear to be from people or sites you trust.
- **Review your credit card and bank account statements often**. If you see charges that you don't recognize, contact your bank or credit card provider right away.

What is PUBLIC data?

It is information that is generally available to the general public. Another way to think of it: Is it OK for this data to be on the front page of the newspaper or on a public website?

Visit the eSecurity Extranet website for previous issues of eSecurity Newsletters

Questions or comments?

E-mail us at eSecurity@state.de.us